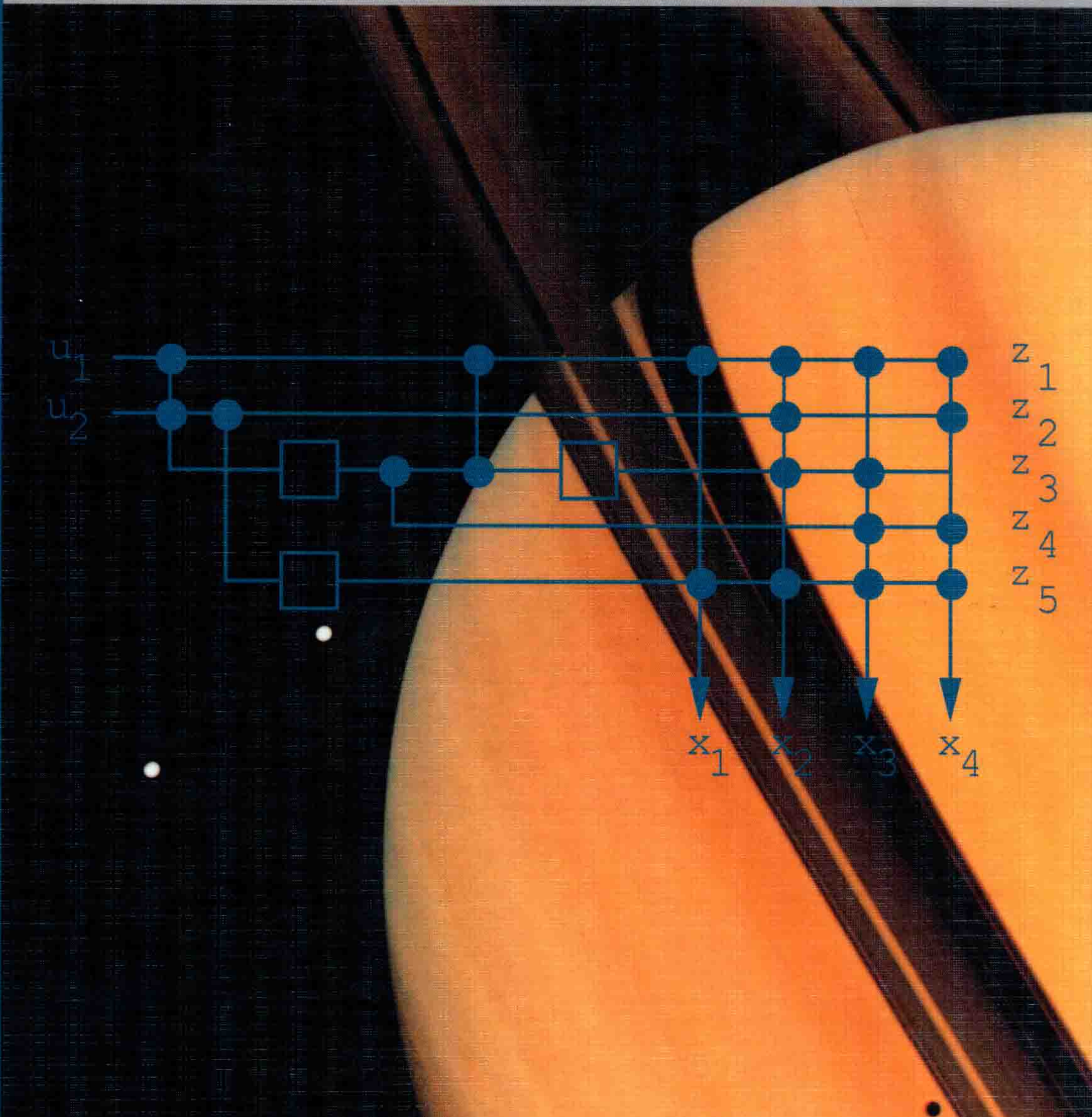

I

Handbook of Coding Theory

V.S. Pless and W.C. Huffman, Editors

NORTH-HOLLAND

Handbook of Coding Theory

VOLUME I

Editors

V.S. Pless
University of Illinois, Chicago, IL, USA

W.C. Huffman
Loyola University, Chicago, IL, USA

R.A. Brualdi (Assistant Editor)
University of Wisconsin, WI, USA

1998

ELSEVIER
Amsterdam · Lausanne · New York · Oxford · Shannon · Singapore · Tokyo

ELSEVIER SCIENCE B.V.
Sara Burgerhartstraat 25
P.O. Box 211, 1000 AE Amsterdam, The Netherlands

Library of Congress Cataloging in Publication Data
A catalog record from the Library of Congress has been applied for.

ISBN: 0-444-81472-8 (Volume I)
ISBN: 0-444-50088-X (Set of volumes I and II)

∞ The paper used in this publication meets the requirements of ANSI/NISO Z39.48-1992 (Permanence of Paper).

Printed in The Netherlands

Handbook of Coding Theory

VOLUME I

About the cover illustration:

Saturn and two of its moons, Tethys (upper) and Dione, as photographed by *Voyager 1* on November 3, 1980, from 13 million kilometers (8 million miles). One of the moons is casting a shadow on the surface of Saturn. The imaging system used a rate 1/2, constraint length-7 convolutional code during the flyby. [Photo provided courtesy of NASA/JPL/Caltech.]

Overlaying Saturn is the circuit design for an encoder of a (4,2) rate1/2 convolutional code.

To my children
Nomi, Ben, and Dan
and grandchildren
Lilah, Evie, and Becky
—V. S. P.

To Gayle, Kara, and Jonathan
Thanks for all your love and support
—W. C. H.

Preface

As a mathematical theory, coding theory is very young, with its roots in Shannon's seminal 1948 paper. The practical gains, due to coding, demonstrated there, and elsewhere since, have provided motivation for much of coding theory. It is fascinating how a large mathematical theory was and is continuing to be developed. The mathematical areas needed in classical coding have been mainly algebraic. As the chapters of this Handbook show, subsequent developments have expanded this mathematical theory considerably.

A frequent question in coding theory is how does one construct a code, or structure related to a code, that is optimal in some mathematical or applied sense. Much of this handbook is devoted to discovering what optimal means in different contexts, finding codes or related structures that are optimal or nearly optimal, and then exploring and exploiting their properties.

Chapter 1 of the Handbook was written by the editors to present the foundations of algebraic coding theory and to provide a unified terminology and set of basics for the other chapters. This chapter, along with many of the others, is accessible to graduate students in mathematics, computer science, and electrical engineering. The audience for this Handbook can range from an active researcher in coding theory to someone beginning to explore this far reaching subject.

The Handbook is divided into three parts, the first part comprising Volume I and the remaining two parts Volume II. Part 1, *Algebraic Coding*, deals primarily with the algebraic structure of error correcting codes. Part 2, *Connections*, is devoted to connections between coding theory and other branches of mathematics and computer science. Part 3, *Applications*, deals with a variety of applications of coding. The authors have taken a broad perspective on their topics, and, by interacting with other authors, have often established links between the chapters. Most of the chapters are self-contained with the majority of the proofs presented in full. Open problems are often identified, and many chapters bring you to the frontiers of research. Each chapter provides an extensive bibliography that will be a tool to extend the development of that chapter.

The reader will discover topics such as complexity, code bounds, and decoding covered both in chapters devoted to these subjects and also as parts of other chapters. Some other topics are also not covered in a single chapter but are presented from many contexts in several chapters. The extensive index at the end of each volume will lead the reader to topics of interest.

We thank the authors not only for their chapters but for many suggestions which have improved the Handbook. We thought the following summaries might help our readers.

Chapter 2 describes many combinatorial constructions of linear codes to aid in constructing codes with certain properties or show that codes with certain parameters cannot exist. Standard constructions such as shortening, extending, using residual codes, and obtaining new codes from old are treated. Properties of weights in even codes are presented. Relations between codes are explored in greater depth for binary self-dual codes where parents, children and neighbors are explained. Contracted codes give different kinds of relations between self-dual codes based on an element in the group of the code being contracted. The discussion of circulant codes is facilitated by giving elementary constructions of generating idempotents of quadratic residue codes over GF(2), GF(4), GF(3), and GF(9). Constructions are also given for the family of greedy codes.

Self-dual codes, the subject of Chapter 3, are important because many of the best known codes are of this type, and they have a rich mathematical theory. Topics in this chapter deal with codes over GF(2), GF(3), GF(4), GF(q), $\mathbb{Z}_4$, and $\mathbb{Z}_m$. Weight enumerators of all the possible varieties are given and the bases for these enumerators are found using invariant theory. Where relevant, shadow codes are explored. Bounds for the highest weights of the various codes are derived leading to a new definition of extremal codes. The theory of the classification of self-dual codes is discussed giving "mass formulas" and explaining "gluing". Tables are presented for self-dual codes giving the codes known of highest minimum weight. There is a comprehensive bibliography.

In the next two chapters, 4 and 5, tables of the best known codes are presented. Chapter 4 is devoted to linear codes, while Chapter 5 considers the best binary codes, either linear or nonlinear. In each chapter, appropriate bounds and construction techniques are developed which will assist the reader in understanding the tables. Chapter 4 presents upper and lower bounds on the highest possible minimum distance d of an $[n, k]$ linear code over GF(q) where n and k are within specified ranges which depend on q; for example when $q = 2$, all n and k with $1 \leqslant k \leqslant n \leqslant 256$ are considered. Tables are given for q up through 9. Chapter 4 also gives tables related to codes meeting the Griesmer bound and tables bounding the number of rational points on algebraic curves of genus up to 50 over certain fields of characteristic 2 or 3. Chapter 5 presents tables of the minimum known redundancy of an (n, M, d) binary code for $1 \leqslant n \leqslant 512$ and $3 \leqslant d \leqslant 29$ with d odd.

Chapter 6 deals with universal bounds for codes and designs in compact metric spaces. These bounds are valid for all codes and designs in the spaces under consideration. General universal bounds for codes and designs are obtained using solutions of some extremum problems for systems of orthogonal polynomials and expressed via parameters of the systems. For finite metric spaces which are P- and Q-polynomial association schemes, a duality in bounding the optimal sizes of codes and designs is found. This gives rise to three pairs of universal bounds for codes and designs in such spaces. For the spaces of primary interest in coding theory, namely, Hamming space, Johnson space, the unit Euclidean sphere, and projective space, these general bounds are calculated and their asymptotic behavior is given.

In Chapter 7 the emphasis is on the theoretical performance limits of the best known codes. Therefore, the main subjects of the chapter are families of asymptotically good codes, that is codes whose rate and relative distance are nonvanishing fractions of the code length n. From a coding-theoretic point of view, algorithmic problems that are studied in the chapter are concerned with constructing good codes, encoding and decoding them, and computing important numerical parameters of the codes. From the computation-theoretic point of view, algorithmic problems can be classified into easy, i.e. polynomial in n, difficult (exponential), and intractable (for instance, NP-complete). Therefore, one has to study the best achievable performance of linear codes under various complexity restrictions. Accordingly, the chapter consists of three main parts, dealing with polynomial algorithms for decoding and construction of asymptotically good codes, exponential algorithms for maximum likelihood decoding and computing some parameters of codes, and NP-complete coding problems.

Two fundamental problems for the covering radius are explored in Chapter 8. The first is to find a "covering" code of length n and covering radius r of smallest dimension $k(n, r)$. The second is to find a code of length n and dimension k whose covering radius $t(n, k)$ is minimized. Knowledge of the t-function is equivalent to knowledge of the length function $l(m, r)$, which is the smallest length of a code with codimension m and covering radius r. Theoretical results on these functions are developed for linear binary codes, for nonlinear binary codes and, to a lesser extent, for codes over other finite fields. Tables of lower and upper bounds for $k(n, r)$ and $l(m, r)$ are included. In addition, upper and lower bounds on the covering radius abound, and many constructions are given for both nonlinear and linear codes. Normal codes are considered to facilitate the use of these constructions. Results and tables are given on the covering radius of specific families of codes including extremal self-dual codes, Reed–Muller codes, and BCH codes. Relations between the covering radius of a code and subcodes are explored as are orphans. Various asymptotic results involving the covering radius can also be found.

The final four chapters of Volume I concentrate on four specific classes of codes: quadratic residue, algebraic geometry, cyclic, and convolutional codes.

Chapter 9 presents generalized quadratic residue codes of prime power lengths as group algebra codes, and inspired by properties of these codes, the author develops the basic ideas of divisibility for codes. The chapter includes a proof of the Gleason–Prange theorem on automorphisms of quadratic residue codes using induced representations of the special linear group. In the divisible code context, the chapter contains a proof of the Gleason–Pierce theorem on formally self-dual codes and a theorem of MacWilliams on equivalences of codes. There is also a description of quadratic residue codes of square lengths as connected with inversive planes and a characterization of constant-weight linear codes.

Chapter 10 gives a survey of the now classical treatment of algebraic geometry codes. The theory of these codes is rather involved and deep. A large part of the theory of modular curves is required to understand the existence of asymptotically good sequences of codes on these curves. The decoding procedure called "majority voting for unknown syndromes" gives a new bound for the minimum distance of algebraic geometry codes and is the starting point of an elementary treatment of these codes and the foundation of the main part of this chapter. The key concept, which is well-known in the context of computational algebra and Gröbner bases, is that of an order function. This approach results in an explicit and easy description of asymptotically good sequences of curves over GF(q) when q is a square. It also gives a self-contained and elementary construction and decoding of algebraic geometry codes.

Chapter 11 examines several famous, and often old, problems dealing with cyclic and extended cyclic codes. Techniques involving group algebras, Fourier transforms, polynomials over finite fields, and solving algebraic systems shed light on these problems. The codes considered include primitive, nonprimitive, simple-root, repeated-root, affine-invariant, and BCH codes. The problems examined include finding weight enumerators, describing the form of codewords, and finding minimum distance. The involvement of cyclic codes in cryptology and in the description of Goppa, Kerdock and Preparata codes is also studied.

It is appropriate that the first volume end with a chapter on convolutional codes as they play such a significant role in applications, the subject of the second half of Volume II. Convolutional codes were invented in the fifties and became widespread in practice when it was discovered in the late sixties that they could be decoded by Viterbi decoding. However, the theory lagged until the seventies when Forney showed that the algebra of $k \times n$ matrices over the field of rational functions in the delay operator played the same role for convolutional codes as the algebra of $k \times n$ matrices over a finite field plays for linear block codes. This chapter introduces new terminology and greatly clarifies this complex algebra. A series of examples is maintained from section to section to assist the reader in understanding the theory as it is developed.

The first chapter of Part 2 (*Connections*) illustrates the usefulness of number theory as a tool in many coding theoretical problems. For example, the authors show how to use character sums and systems of equations over abelian groups and finite fields to study the minimum distance and covering radius of a code. Number theoretical methods are also used to study cyclic codes such as BCH codes and their duals. In addition, the problem of finding perfect codes is examined and complete proofs are presented of the results classifying the parameters that lead to perfect codes.

As stated earlier, the mathematical foundation of coding theory goes back to Claude Shannon's fundamental work in the forties. Cryptology also has its foundations in Shannon's work. Chapter 14 describes the connection between cryptology and coding theory. After a general introduction to cryptology, this chapter discusses shift register systems and the use of the Berlekamp–Massey decoding algorithm in cryptology. Public key cryptosystems based on the complexity of decoding block codes and authentication codes and their relation to block codes are described, as are relations between the wiretap channel and generalized Hamming weights, and between threshold schemes and MDS codes.

Combinatorial designs have intimate connections with codes, arising in particular as the supports of codewords of a given weight. Chapter 15 explores a multitude of these connections including designs arising from codes which are optimal according to a variety of bounds. The study covers t-designs, resolvable designs, orthogonal arrays, and quasi-symmetric designs arising from codes, and conversely, codes arising from designs and Hadamard matrices. With majority-logic, designs supported by a linear code can be used for decoding of the dual code.

Continuing with the relationship between codes and designs, Chapter 16[1] gives a treatment of the Reed–Muller and generalized Reed–Muller codes, with a particular emphasis on those that are associated with the combinatorial designs defined by finite geometries. The codes are first defined as polynomial functions in multiple variables, and their association with the designs from finite geometries is described. Alternative treatments of the

[1] See postscript, at end of preface.

codes as group algebras of elementary abelian p-groups or as extended cyclic codes are described, along with some of the main theorems linking these different approaches. In particular, the Mattson–Solomon polynomial is used to relate generalized Reed–Muller codes to the radical of the group algebra. The use of Reed–Muller codes in majority-logic decoding is included.

Chapter 17 examines the connection between codes and groups. From a code there naturally arises a group, the automorphism group. Conversely, given a group, one can find a code either associated with the group algebra or as a space invariant under the group. Using a variety of techniques developed by a number of authors, the bulk of this chapter presents the theory leading to the construction of the automorphism groups of major families of codes: Cauchy, generalized Reed–Solomon, affine invariant, generalized Reed–Muller, BCH, and generalized quadratic residue codes. The judicious selection of automorphisms provides a tool for decoding a code using permutation decoding and a tool for decomposing codes into particularly nice subcodes.

The interplay between codes and association schemes had its primary stimulus in the 1973 work of Delsarte. Chapter 18 expands on this work and that of succeeding authors. The duality of association schemes, the MacWilliams transform, and the Pless power moments identities are investigated in the setting of Hamming schemes and in more general settings as well. The chapter focuses on abelian schemes, but some attention is also paid to nonabelian association schemes.

The central thread of the first chapter of Part 3 (*Applications*) is a discussion of the class of decoders arising in a process known as "locator decoding". These decoders are by far the most useful in practice. This class of decoders partitions the decoding problem into two parts: first find which components of the received message are in error, and then find the values of the errors. The two topics can be studied separately, and there are many algorithms for doing this; their common feature is the use of the error-locator polynomial. Codes most suitable for locator decoding are those codes that are based on the BCH bound; these are the Reed–Solomon codes and their subfield-subcodes, the BCH codes. Many of the decoding algorithms depend on properties of the Fourier transform (described in an appendix). The task of decoding Reed–Solomon codes is generalized to the tasks of decoding two dimensional bicyclic codes and the decoding of Hermitian codes. This chapter is concerned with explicit constructions of practical decoders.

Chapter 20 develops the theory and practice of code design for input-constrained channels, such as magnetic and optical data recording channels. The purpose of these codes is to improve the performance of the channel by matching the characteristics of the recorded signals to those of the channel. Finite-state encoders are described and an algorithm presented which gives a rigorous procedure for designing these encoders which are used to encode arbitrary user sequences into the constrained sequences that are actually recorded on the channel. For a wide class of useful constraints, these encoders are sliding-block decodable which means that decoding has limited error propagation. Other methods of encoder construction are described within the mathematical framework of this chapter. Several results bearing on complexity issues and finite procedures for encoders are also presented.

Chapter 21 deals with sequences having desirable correlation properties, commonly referred to as pseudorandom sequences. The list of sequences/sequence families discussed includes Barker, bent function, four-phase, GMW, Gold, Kasami, maximum length, No and optical orthogonal code sequences. Bounds on attainable correlation magnitudes are included. The chapter brings out the strong ties between sequences having low periodic correlation and coding theory. Often the dual of an efficient error-correcting code will yield a family of low correlation sequences. The reader will find in this chapter a detailed discussion of the $\mathbb{Z}_4$-linear versions of the Kerdock, Preparata, Delsarte–Goethals and Goethals codes, including an explanation for the apparent duality exhibited by the binary Kerdock and Preparata codes.

Array codes, the subject of Chapter 22, deal essentially with errors of 2-dimensional type in media like multi-track magnetic recording and holographic storage. These are useful codes when the channel is subject to burst errors. Block, convolutional, and maximum rank array codes are studied as are the related CIRC codes used in compact disk technology. Specific families of array codes are constructed throughout the chapter. Decoding techniques to correct both errors and erasures are explored.

Concatenated codes and their multilevel generalizations are described in Chapter 23. By combining two or more different codes of lengths n and N, concatenated techniques build up efficient codes of length nN. In fact, there exist asymptotic families of concatenated codes with linearly increasing distance and polynomial construction complexity. Multilevel concatenated codes have very good parameters for their comparatively short block lengths. The chapter presents concatenated constructions in Hamming and Euclidean spaces, discusses asymptotic properties and studies bounded distance decoding.

A trellis T is an edge-labeled directed graph with the property that every vertex in T has a well-defined depth. Trellises were first introduced by Forney in the sixties to better explain the Viterbi algorithm for decoding convolutional codes, and trellis decoding algorithms remain the primary motivation for research on the trellis structure of block codes. Chapter 24 gives a brief elementary introduction to this topic and the Viterbi algorithm.

The final chapter of the Handbook describes the "match made in heaven" between deep space telecommunications and coding theory. The chapter gives both a technical and historical account of the use of codes beginning with the 1969 *Mariner* journeys to Mars, continuing with the *Pioneer* and *Voyager* missions, and concluding with the *Galileo* and *Cassini* projects. The telemetry channel link budget and coding gain are discussed in connection with the evolving CCSDS coding standard. A variety of codes were used including Reed–Muller, extended Golay, convolutional, and concatenated codes working in conjunction with decoding techniques involving the Fast Hadamard Transform, the Big Viterbi Decoder, and turbo decoders.

Postscript

While this Handbook was in press, the editors were saddened to hear Ed Assmus had died suddenly at Oberwolfach on 18 March 1998. Ed looked forward with great anticipation to the publication of this Handbook. His contributions to coding theory and design theory, along with their various interconnections, will remain important for many years to come. Many results in these areas bear his name, and his recent book with Jenny Key has stimulated much research. He will be missed by all in our community.

Vera S. Pless
W. Cary Huffman

List of Contributors

Assmus, E.F., Jr., *Lehigh University, Bethelehem, PA* (Ch. 16).
Barg, A., *Bell Laboratories, Lucent Technologies, Murray Hill, NJ* (Ch. 7).
Blahut, R.E., *University of Illinois, Urbana, IL* (Ch. 19).
Blaum, M., *IBM Research Division, Almaden Research Center, San Jose, CA* (Ch. 22).
Brouwer, A.E., *Eindhoven University of Technology, Eindhoven* (Ch. 4).
Brualdi, R.A., *University of Wisconsin, Madison, WI* (Chs. 1, 8).
Camion, P., *INRIA–Rocquencourt, Le Chesnay Cedex* (Ch. 18).
Charpin, P., *INRIA–Rocquencourt, Le Chesnay Cedex* (Ch. 11).
Dumer, I., *University of California at Riverside, Riverside, CA* (Ch. 23).
Farrell, P.G., *University of Manchester, Manchester, UK* (Ch. 22).
Helleseth, T., *University of Bergen, Bergen* (Ch. 21).
Høholdt, T., *Technical University of Denmark, Lyngby* (Ch. 10).
Honkala, I., *University of Turku, Turku* (Ch. 13).
Huffman, W.C., *Loyola University, Chicago, IL* (Chs. 1, 17).
Key, J.D., *Clemson University, Clemson, SC* (Ch. 16).
Kumar, P. Vijay, *University of Southern California, Los Angeles, CA* (Ch. 21).
Levenshtein, V.I., *Keldysh Institute for Applied Mathematics, Russian Academy of Sciences, Moscow* (Ch. 6).
Lint, J.H. van, *Eindhoven University of Technology, Eindhoven* (Ch. 10).
Litsyn, S., *Tel-Aviv University, Ramat-Aviv* (Chs. 5, 8).
Marcus, B.H., *IBM Research Division, Almaden Research Center, San Jose, CA* (Ch. 20).
McEliece, R.J., *California Institute of Technology, Pasadena, CA* (Ch. 12).
Pellikaan, R., *Eindhoven University of Technology, Eindhoven* (Ch. 10).
Pless, V.S., *University of Illinois–Chicago, Chicago, IL* (Chs. 1, 2, 8).
Rains, E.M., *AT&T Labs-Research, Florham Park, NJ* (Ch. 3).
Roth, R.M., *Technion – Israel Institute of Technology, Haifa* (Ch. 20).
Siegel, P.H., *University of California at San Diego, La Jolla, CA* (Ch. 20).
Sloane, N.J.A., *AT&T Labs-Research, Florham Park, NJ* (Ch. 3).
Tietäväinen, A., *University of Turku, Turku* (Ch. 13).
Tilborg, H.C.A. van, *Eindhoven University of Technology, Eindhoven* (Chs. 14, 22).
Tonchev, V.D., *Michigan Technological University, Houghton, MI* (Ch. 15).
Vardy, A., *University of Illinois, Urbana, IL* (Ch. 24).
Ward, H.N., *University of Virginia, Charlottesville, VA* (Ch. 9).
Wicker, S.B., *Cornell University, Ithaca, NY* (Ch. 25).

Contents

Volume I

Volume II

Part 2: Connections

Part 3: Applications

Part 1
Algebraic Coding